Available online at www.sciencedirect.com

SCIENCE DIRECT

Discrete Mathematics 306 (2006) 2038–2046

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Varieties of algebras arising from K-perfect m-cycle systems

Robert Brier, Darryn Bryant

Department of Mathematics, University of Queensland, Qld. 4072, Australia

Received 26 September 2004; received in revised form 28 March 2006; accepted 12 April 2006
Available online 14 June 2006

Abstract

A class of algebras forms a variety if it is characterised by a collection of identities. There is a well-known method, often called the standard construction, which gives rise to algebras from m-cycle systems. It is known that the algebras arising from $\{1\}$-perfect m-cycle systems form a variety for $m \in \{3, 5\}$ only, and that the algebras arising from $\{1, 2\}$-perfect m-cycle systems form a variety for $m \in \{3, 5, 7\}$ only. Here we give, for any set K of positive integers, necessary and sufficient conditions under which the algebras arising from K-perfect m-cycle systems form a variety.

Keywords: Homomorphism; K-perfect m-cycle system; m-circuit system; Variety

1. Introduction

An algebra $\mathscr{A}=(A, f_1, f_2, \ldots, f_t)$ consists of a set A together with functions $f_1, f_2, \ldots, f_t$, where for $i=1, 2, \ldots, t$, there is a non-negative integer n_i, and f_i maps A^{n_i} to A. The function f_i is called an n_i-*ary operation*. We will be concerned only with binary operations. A class $\mathscr{V}$ of algebras is a *variety* when it is characterised by a set of identities. That is, there exists a set Σ of identities such that $\mathscr{A} \in \mathscr{V}$ if and only if $\mathscr{A}$ satisfies each of the identities in Σ. A fundamental theorem of universal algebra, see [1], says that a class of algebras forms a variety if and only if it is closed under taking of direct products, subalgebras and homomorphic images.

A *groupoid* is an algebra $(S, *)$ with one binary operation. The binary operation is sometimes denoted by juxtaposition with the symbol $*$ being omitted, but we will include the symbol whenever confusion is possible. The class of all groupoids forms a variety defined by the empty set of identities. We say that a groupoid in which $xa = b$ has a unique solution for all $a, b \in S$ is *column latin*, and a groupoid in which $ax = b$ has a unique solution for all $a, b \in S$ is *row latin*. A *quasigroup* is a groupoid that is both row and column latin. An *algebraic quasigroup* is an algebra $(Q, *, /, \backslash)$ in the variety defined by the following four identities.

$$(xy)/y = x,$$
$$(x/y)y = x,$$
$$y\backslash(yx) = x,$$
$$y(y\backslash x) = x.$$

E-mail address: rbrier@maths.uq.edu.au (R. Brier).

0012-365X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.04.002

If $(Q, *, /, \backslash)$ is an algebraic quasigroup then $(Q, *)$ is a quasigroup. The unique solution to $xa = b$ is b/a, and the unique solution to $ax = b$ is $a\backslash b$. Conversely, given any quasigroup $(Q, *)$, one can construct an algebraic quasigroup $(Q, *, /, \backslash)$ by defining, for all $a, b \in Q$, b/a to be the unique solution to $xa = b$, and $a\backslash b$ to be the unique solution to $ax = b$.

There is a well-known method for constructing groupoids, and sometimes quasigroups, from certain decompositions of graphs into circuits, but to describe it we first need the following concepts. Let G be a simple graph. A *circuit* in G is a closed walk in G with no repeated edges. The *length* of a circuit is the number of edges it contains, and a circuit of length m is called an *m-circuit*. We do not distinguish the first vertex of a circuit, or the direction (forwards or backwards) in which it is traversed. Thus, we may denote the m-circuit which traverses, in order, the edges $v_1v_2, v_2v_3, \ldots, v_{m-1}v_m, v_mv_1$ by $(v_1, v_2, \ldots, v_m)$ or $(v_m, v_{m-1}, \ldots, v_1)$ or by any cyclic permutation of either of these. Note, however, that the order in which the edges are traversed is important. For example, the following two 6-circuits traverse the same edges but are distinct.

$$(1, 2, 3, 1, 4, 5) \quad (1, 2, 3, 1, 5, 4).$$

A *circuit system of order n* is a pair $(S, \mathscr{C})$ where S is a set of cardinality n and $\mathscr{C}$ is a set of circuits such that every edge of the complete graph on S is traversed by exactly one circuit in $\mathscr{C}$ (note that S can have infinite cardinality). If all the circuits in $\mathscr{C}$ are m-circuits, then $(S, \mathscr{C})$ is an *m-circuit system*. A circuit system $(S, \mathscr{C})$ gives rise to a groupoid $(S, *)$ if we define a binary operation $*$ on S as follows:

- For all $x \in S$, $x * x = x$.
- For distinct $x, y \in S$, $x * y = z$ and $y * x = w$ where $(\ldots, w, x, y, z, \ldots)$ is the unique circuit in $\mathscr{C}$ containing the edge xy.

This method of constructing the binary operation $*$ on the underlying set of a circuit system is usually called the *standard construction* and was introduced by Kotzig in [8].

Clearly, the groupoid $(S, *)$ arising from a circuit system satisfies the identities $x^2 = x$ and $(xy)y = x$. The second identity ensures that the groupoid is column latin. There is a nice characterisation of when these groupoids are also row latin, and hence give rise to quasigroups, but to describe it we first need the notion of *K-perfect*, which we now define.

Given an m-circuit $C = (v_1, v_2, \ldots, v_m)$ and an integer k, we denote by $C(k)$ the graph with vertex set $\{v_1, v_2, \ldots, v_m\}$ and edge set $\{v_iv_{i+k} : i = 1, 2, \ldots, m\}$ (the subscripts being reduced modulo m on the residues $1, 2, \ldots, m$). Note that $|E(C(k))| = m$. Note also that for $k > 1$, $C(k)$ may contain loops and/or multiple edges. If $\mathscr{C}$ is a collection of circuits then we define $\mathscr{C}(k) = \{C(k) : C \in \mathscr{C}\}$. We say that a circuit system $(S, \mathscr{C})$ is *k-perfect* if the graphs in $\mathscr{C}(k)$ partition the edge set of the complete graph on S. Let K be a set of integers. We say that a circuit system is *K-perfect* if it is k-perfect for each $k \in K$.

Given an m-circuit $C = (v_1, v_2, \ldots, v_m)$ and vertices u and v, if $u = v_i$ and $v = v_{i+k}$ we say that the walk $v_i, v_{i+1}, \ldots, v_{i+k}$ is a *C-walk of length k* between u and v, and also between v and u. It is clear that the number of times the edge uv occurs in $C(k)$ is the number of different C-walks of length k between u and v. Given a collection of circuits $\mathscr{C}$, we say that a *$\mathscr{C}$-walk* exists between u and v if a C-walk exists between u and v for some $C \in \mathscr{C}$. It is clear that a circuit system $(S, \mathscr{C})$ is k-perfect if and only if there is exactly one $\mathscr{C}$-walk of length k between each pair of vertices.

If an m-circuit system $(S, \mathscr{C})$ is k-perfect, then clearly it is also $(m - k)$-perfect and $(m + k)$-perfect. It is also clear that every m-circuit system is 1-perfect and no m-circuit system is $m/2$-perfect. Hence, when considering m-circuit systems, it suffices to consider $K \subseteq \{1, 2, \ldots, \lfloor (m - 1)/2 \rfloor\}$ with $1 \in K$.

Now, let $(S, \mathscr{C})$ be a K-perfect circuit system and let $(S, *)$ be the groupoid arising from $(S, \mathscr{C})$ via the standard construction. We inductively define words in the variables x and y by $W_0(x, y) = x$, $W_1(x, y) = y$, and $W_i(x, y) = W_{i-2}(x, y) * W_{i-1}(x, y)$ for all $i \geqslant 2$. For $i < 0$ $W_i(x, y)$ is also well defined because

$$W_{i-1} = (W_{i-1}(x, y) * W_i(x, y)) * W_i(x, y) = W_{i+1}(x, y) * W_i(x, y).$$

For any distinct $a, b \in S$, the unique circuit in $\mathscr{C}$ traversing the edge ab is given by

$$(W_0(a, b), W_1(a, b), \ldots, W_{m-1}(a, b)),$$

where m is the length of the circuit. This notation was introduced in [5]. For each $k \in K$ we can now define a binary operation $\backslash_k$ as follows:

- For all $a \in S$, $a \backslash_k a = a$.
- For all distinct $a, b \in S$, $a \backslash_k b$ is the unique solution to $W_k(a, x) = b$.

Notice that $W_k(a, x) = b$ does indeed have a unique solution. The edge ab is in $C(k)$ for some unique circuit $C \in \mathscr{C}$, and if

$$C = (\ldots, a, u_1, u_2, \ldots, u_{k-1}, b, \ldots)$$

then u_1 is the unique solution.

It is well known, and straightforward to prove, that the groupoid arising from a circuit system $(S, \mathscr{C})$ is row latin if and only if $(S, \mathscr{C})$ is 2-perfect [8]. Thus, if $(S, \mathscr{C})$ is a 2-perfect circuit system we can construct an algebraic quasigroup $(S, *, /, \backslash)$ where $* = /$ is the binary operation given by the standard construction, and $\backslash$ is the binary operation $\backslash_2$ defined above.

It is natural to generalise these ideas as follows. Let $K = \{k_1, k_2, \ldots, k_t\}$ be any subset of $\{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$, and let $(S, \mathscr{C})$ be a K-perfect m-circuit system. We construct an algebra $(S, *, \backslash_{k_1}, \backslash_{k_2}, \ldots, \backslash_{k_t})$, which we call the *algebra arising from the K-perfect circuit system* $(S, \mathscr{C})$. Here, $*$ is the binary operation given by the standard construction, and $\backslash_{k_1}, \backslash_{k_2}, \ldots, \backslash_{k_t}$ are the binary operations defined above. As an abbreviation we will denote the algebra $(S, *, \backslash_{k_1}, \backslash_{k_2}, \ldots, \backslash_{k_t})$ as $(S, *, \backslash_K)$ where $K = \{k_1, k_2, \ldots, k_t\}$. Of course $\backslash_K$ is not itself an operation.

The underlying graph of an m-circuit $C = (v_1, v_2, \ldots, v_m)$ (equivalently the graph $C(1)$) in which $v_1, v_2, \ldots, v_m$ are distinct is an m-cycle. Thus, we call an m-circuit system $(S, \mathscr{C})$ an *m-cycle system* if $v_1, v_2, \ldots, v_m$ are distinct for each m-circuit $(v_1, v_2, \ldots, v_m) \in \mathscr{C}$. The technical difference between our definition of m-cycle system and the usual definition, in which the elements of $\mathscr{C}$ are m-cycles rather than walks around them, is of no consequence. For all $m \geqslant 3$ and any subset K of $\{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$, we define $\mathbf{C}_m^K$ to be the class of algebras arising from all K-perfect m-cycle systems (of both finite and infinite order).

The purpose of this paper is to give a complete solution to the question of when $\mathbf{C}_m^K$ is a variety. As such we prove the following theorem.

Theorem 1.1. *Let $m \geqslant 3$ be an integer and let $K \subseteq \{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$. The class $\mathbf{C}_m^K$ is a variety if and only if*

- $m \neq 4$,
- $m \not\equiv 2 \pmod 4$, *and*
- *for all t in the range $1 \leqslant t < m/2$, at least one of t, $t/2$ or $(m-t)/2$ is in K.*

Moreover, when $\mathbf{C}_m^K$ is a variety it is defined by the following identities:

$$\begin{aligned} x^2 &= x, \\ (xy)y &= x, \\ W_m(x, y) &= x, \\ x \backslash_k W_k(x, y) &= y \quad \text{for all } k \in K, \\ W_k(x, x \backslash_k y) &= y \quad \text{for all } k \in K. \end{aligned}$$

It follows immediately from this theorem that $\mathbf{C}_m^{\{1\}}$ is a variety for $m \in \{3, 5\}$ only, and that $\mathbf{C}_m^{\{1,2\}}$ is a variety for $m \in \{3, 5, 7\}$ only. These results are well known, see [5,6]. Also see [2–4,7,9–12] for related results.

2. Some existence results

In this section we will show that certain K-perfect m-circuit systems exist by using methods from [12]. To use the methods we need to introduce a number of definitions. An *edge coloured graph* G^* is a graph G, which may contain parallel edges but does not contain loops, along with an assignment of colours to the edges G. We denote by rK_n^* the

graph with n vertices and with exactly one edge of each of r colours between each pair of vertices. Two edge coloured graphs G^* and H^* are *isomorphic* if there is a bijection $\phi : V(G^*) \to V(H^*)$ such that the edge ab is in G^* if and only if the edge $\phi(a)\phi(b)$ is in H^*, and ab and $\phi(a)\phi(b)$ are assigned the same colour in G^* and in H^*. An edge coloured G^*-*decomposition* of rK_n^* is an edge disjoint collection of edge coloured subgraphs of rK_n^*, each isomorphic to G^*, whose edge sets partition the edge set of rK_n^*. When we wish to identify the set S of vertices of rK_n^* and the set $\mathscr{G}^*$ of edge coloured subgraphs, we write the edge coloured G^*-decomposition as a pair $(S, \mathscr{G}^*)$. We will use the following theorem and corollary from [12].

Theorem 2.1 (*Li Marzi et al. [12]*). *Let G^* be an edge coloured subgraph of rK_n^* with the property that each of the r colours is assigned to exactly m edges of G. Suppose there exists an assignment of the integers $1, 2, 3, \ldots, m$ to the edges of G such that*:

- *parallel edges are assigned the same integer, and*
- *for each colour α, the integers assigned to the edges coloured α are distinct.*

Then there exists an edge coloured G^*-decomposition of rK_q^* for all sufficiently large prime powers $q \equiv 1 \pmod{2m}$.

Corollary 2.1 (*Li Marzi et al. [12]*). *If G^* is a simple edge coloured subgraph of rK_n^* with each of the r colours assigned to m edges of G then there exists an edge coloured G^*-decomposition of rK_q^* for all sufficiently large prime powers $q \equiv 1 \pmod{2m}$.*

In [12], the next corollary was only stated for $K = \{1, 2, 3\}$, but essentially the same proof gives the result for general K.

Corollary 2.2. *Let m be a positive integer and let $K \subseteq \{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$. There exists a K-perfect m-cycle system of order q for all sufficiently large prime powers $q \equiv 1 \pmod{2m}$.*

Proof. Let C be an m-cycle. Let $r = |K|$ and let $\{\alpha_k \mid k \in K\}$ be a set of r distinct colours. For each $k \in K$, let $C^*(k)$ be $C(k)$ with all of its edges coloured α_k. Let C^* be the edge coloured graph with vertex set $V(C)$ and edge set $\bigcup_{k\in K} E(C^*(k))$. Clearly C^* is a simple subgraph of rK_m^*, with m edges of each of the r colours. Hence by Corollary 2.1, there is an edge coloured C^*-decomposition $(S, \mathscr{C}^*)$ of rK_q^* for all sufficiently large prime powers $q \equiv 1 \pmod{2m}$. Let $\mathscr{C}^* = \{C_1^*, C_2^*, \ldots, C_t^*\}$ and for $i = 1, 2, \ldots, t$ let C_i be the unique m-cycle whose edges are the edges of colour α_1 in C_i^*. Then it is clear that $(S, \{C_1, C_2, \ldots, C_t\})$ is a K-perfect m-cycle system of order q. □

A $(t, m-t)$-*hourglass* is an m-circuit $(v_1, v_2, \ldots, v_t, v_1, v_{t+1}, v_{t+2}, \ldots, v_{m-1})$, where $v_1, \ldots, v_{m-1}$ are all distinct. For convenience we always assume that $t \leqslant m - t$. Thus for a $(t, m-t)$-hourglass to exist we must have $6 \leqslant 2t \leqslant m$. We call v_1 the *centre point* of $(v_1, v_2, \ldots, v_t, v_1, v_{t+1}, \ldots, v_m)$. A $(t, m-t)$-*hourglass system* is an m-circuit system $(S, \mathscr{C})$ where all the m-circuits in $\mathscr{C}$ are $(t, m-t)$-hourglasses.

Corollary 2.3. *Let m and t be positive integers with $6 \leqslant 2t \leqslant m$ and let K be any subset of $\{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\} \backslash \{t/2, t, (m-t)/2\}$ with $1 \in K$. Then there is a K-perfect $(t, m-t)$-hourglass system of order q for all sufficiently large prime powers $q \equiv 1 \pmod{2m}$.*

Proof. Let $H = (v_1, v_2, \ldots, v_t, v_1, v_{t+1}, \ldots, v_{m-1})$ be a $(t, m-t)$-hourglass. Let $r = |K|$ and let $\{\alpha_k \mid k \in K\}$ be a set of r distinct colours. Let $H^*(k)$ be $H(k)$ with all the edges coloured α_k. For each $k \in K$, let H^* bethe edge coloured graph with vertex set $\{v_1, \ldots, v_{m-1}\}$ and edge set $\bigcup_{k\in K} E(H^*(k))$. There are no loops in H^* because $t \notin K$.

We want to show that H^* is an edge coloured subgraph of rK_n^* for $n \geqslant m - 1$ and that its edges can be labelled with integers so that the conditions of Theorem 2.1 are satisfied. Firstly we will show that any two parallel edges in H^* have v_1 at one of the end points. Choose two parallel edges with end points v_i and v_j and suppose they are assigned colours α_k and α_l. This implies that there are H-walks of length k and l between v_i and v_j. If neither v_i nor v_j is the centre point it follows that $k + l = m$. But then k or $l \geqslant m/2$ which is a contradiction as k and $l \in K$. So all pairs of parallel edges are incident with the centre point.

Now we show that parallel edges have distinct colours, which means that H^* is indeed a subgraph of rK_n^* for $n \geqslant m-1$. Suppose two parallel edges, with end points at v_1 and v_i are assigned the same colour α_k. Since $k < m/2$, it is easy to see that v_i must be opposite v_1 in the t-cycle, or opposite v_1 in the $(m-t)$-cycle. That is, $i = (t+2)/2$ or $i = (m+t)/2$. But then $k = t/2$ or $(m-t)/2$ which is a contradiction.

We now obtain the required labelling for Theorem 2.1. We have seen that every set of parallel edges has v_1 as an end point. There are $m-2$ vertices in H other than v_1, so there are at most $m-2$ sets of parallel edges. For each set X of parallel edges, label all the edges in X with an integer between 1 and $m-2$ inclusive so that distinct sets receive distinct labels. We need to label the remaining edges. Given a specific $k \in K$, consider all the edges of colour α_k, there are m of these. Those which occur in sets of parallel edge have been labelled already, say with integers $\{\beta_1, \ldots, \beta_s\}$. Label the remaining edges of colour α_k with integers from the set $\{1 \ldots, m\} \backslash \{\beta_1, \ldots, \beta_s\}$ so that distinct edges are labelled with distinct integers. By repeating this process for all $k \in K$ we obtain a labelling of H^* which satisfies the conditions of Theorem 2.1.

Hence, by Theorem 2.1 there exists an edge coloured H^*-decomposition $(S, \mathscr{H}^*)$ of rK_q^* for all sufficiently large prime powers $q \equiv 1 \pmod{2m}$. Let $\mathscr{H}^* = \{H_1^*, H_2^*, \ldots, H_t^*\}$ and for $i = 1, 2, \ldots, t$ let H_i be the unique m-circuit whose edges are the edges of colour α_1 in H_i^*. Then it is clear that $(S, \{H_1, H_2, \ldots, H_t\})$ is a K-perfect $(t, m-t)$-hourglass system of order q. □

3. Homomorphisms

An $n \times m$ array is a function, $A : \{1, \ldots, n\} \times \{1, \ldots, m\} \to S$ where S is some set. The ith row of A is the sequence $A(i, 1), \ldots, A(i, m)$ and the jth column of A is the sequence $A(1, j), \ldots, A(n, j)$. We denote the jth column of A by $A[j]$. Two columns $A[i]$ and $A[j]$ are *orthogonal* if put side by side the rows list all the ordered pairs of S, that is $\{(A(1, i), A(1, j)), \ldots, (A(n, i), A(n, j))\} = S \times S$. We denote this by $A[i] \perp A[j]$. If every pair of columns in A are orthogonal then A is an *orthogonal array*. We call two columns $A[i]$ and $A[j]$ *parallel* if $A(k, i) \neq A(k, j)$ for $k = 1, 2, \ldots, n$. We denote this by $A[i] \| A[j]$. If $A : \{1, \ldots, n\} \times \{1, \ldots, m\} \to \{1, 2, \ldots, N\}$ is an array then the array $A + k : \{1, \ldots, n\} \times \{1, \ldots, m\} \to \{1, 2, \ldots, N\}$ is defined by $(A + k)(i, j) = A(i, j) + k$ reduced modulo N on the residues $\{1, 2, \ldots, N\}$.

Theorem 3.1. *Let $m \geqslant 3$ be an integer, let K be any subset of $\{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$, and let $(S, *, \backslash_K)$ be the algebra arising from a finite K-perfect m-circuit system $(S, \mathscr{C})$. Then there is an algebra arising from a finite K-perfect m-cycle system which has a homomorphism onto $(S, *, \backslash_K)$.*

Proof. Let $s = |S|$. Choose large enough r such that:

- a K-perfect m-cycle system $(R, \mathscr{C}')$ exists with $R = \{1, 2, \ldots, r\}$;
- an orthogonal array $A : \{1, \ldots, r^2\} \times \{1, \ldots, m\} \to R$ exists.

By Theorem 2.1 and [13] such an r exists. We use these to construct a K-perfect m-cycle system of order rs. Then we show it gives rise to an algebra which has a homomorphism onto $(S, *, \backslash_K)$. For each $C = (v_1, \ldots, v_m) \in \mathscr{C}$ we construct an $r^2 \times m$ array A_C which has the following properties:

(i) For $i = 1, 2, \ldots, m$ if $k \in K$ then $A_C[i] \perp A_C[i+k]$ (column indices are reduced modulo m on the residues $1, 2, \ldots, m$)
(ii) If $v_i = v_j$ and $i \neq j$ then $A_C[i] \| A_C[j]$.

We construct A_C from A. Consider vertex $v_i \in C$. If $v_j \neq v_i$ for all $j < i$ then we let $A_C[i] = A[i]$. Otherwise, we find the smallest j such that $v_j = v_i$ and let $A_C[i] = (A + (j-i))[j]$ so that $A_C[i] \| A_C[j]$. We do this for $i = 1, 2, \ldots, m$. Note that any pair of columns of A_C are orthogonal or parallel. Suppose $A_C[i] \not\perp A_C[i+k]$. Then $A_C[i] \| A_C[i+k]$, so $v_i = v_{i+k}$ and hence $k \notin K$. So by contraposition, property (i) holds for A_C. The array A_C also satisfies property (ii) because if $v_i = v_j$ and $i \neq j$ then $A_C[i] = (A + (i-h))[h]$ and $A_C[j] = (A + (j-h))[h]$ where h is the smallest integer such that $v_h = v_i = v_j$. Clearly $(A + (i-h))[h] \| (A + (j-h))[h]$.

On $R \times S$ define a set $\mathscr{D}$ of circuits as follows:

(1) For each $v \in S$, place a copy of $(R, \mathscr{C}')$ on $R \times \{v\}$ and place all these m-cycles in $\mathscr{D}$.
(2) For each circuit $C = (v_1, \ldots, v_m)$ in $\mathscr{C}$ and each row $x_1, \ldots, x_m$ of A_C place the m-cycle $((x_1, v_1), \ldots, (x_m, v_m))$ in $\mathscr{D}$. Property (ii) of A_C ensures that these are indeed cycles.

To show that $(R \times S, \mathscr{D})$ is a K-perfect m-cycle system it is sufficient to show that

- $|\mathscr{D}| = rs(rs-1)/2m$;
- for every pair of vertices (x, u) and $(y, v) \in R \times S$ and each $k \in K$ there is a $\mathscr{D}$-walk of length k from (x, u) to (y, v).

The number of cycles given by (1) is $sr(r-1)/2m$ and the number of cycles given by (2) is $r^2 s(s-1)/2m$, so $|D| = rs(rs-1)/2m$. Let $k \in K$ and $(x, u), (y, v) \in R \times S$. Since $(R, \mathscr{C}')$ is K-perfect there is a $\mathscr{C}'$-walk of length k from x to y, let it be $v_1, \ldots, v_{k+1}$. If $u = v$ then $(v_1, u), (v_2, u), \ldots, (v_{k+1}, u)$ is a $\mathscr{D}$-walk of length k from (x, u) to (y, v). If $u \neq v$, there is a $\mathscr{C}$-walk of length k between u and v for some $C \in \mathscr{C}$ as $(S, \mathscr{C})$ is K-perfect. Suppose the C-walk is $u_i, \ldots, u_{i+k}$. By property (i) of A_C, $A_C[i] \perp A_C[i+k]$ so we can find a row $x_1, \ldots, x_m$ of A_C such that $x_i = x$ and $x_{i+k} = y$. Then $(x_i, u_i), (x_{i+1}, u_{i+1}), \ldots, (x_{i+k}, u_{i+k})$ is a $\mathscr{D}$-walk of length k from (x, u) to (y, v). So $(R \times S, \mathscr{D})$ is a K-perfect m-cycle system.

Let $(R \times S, *, \backslash_K)$ be the algebra arising from the standard construction on $(R \times S, \mathscr{D})$. It is straightforward to show that $\phi : R \times S \to S$ defined by $\phi(x, v) = v$ is the required homomorphism. □

4. Main results

The following lemma gives five properties of W_i which we use in this section.

Lemma 4.1. *Let $(S, *, \backslash_K)$ be an algebra arising from a K-perfect circuit system and let i and j be integers.*

(i) $W_i(W_j(x, y), W_{j+1}(x, y)) = W_{i+j}(x, y)$,
(ii) *if* $W_m(x, y) = x$ *for all* $x, y \in S$ *then* $W_{i+m}(x, y) = W_i(x, y)$ *for all* $x, y \in S$,
(iii) $W_i(x, y) = W_{1-i}(y, x)$,
(iv) $W_i(W_j(x, y), W_{j-1}(x, y)) = W_{j-i}(x, y)$,
(v) $W_i(x, x) = x$ *for all* $x \in S$.

Proof. (i) This property was proven in [5].

(ii) $W_i(x, y) = W_m(W_i(x, y), W_{i+1}(x, y))$ since $W_m(x, y) = x$ for all $x, y \in S$
$= W_{i+m}(x, y)$ by Property (i).

(iii) We use induction on i to prove this property. The property holds for $i = 0$ as $W_0(x, y) = x = W_1(y, x)$. Suppose the property holds for $i = k$ so $W_k(x, y) = W_{1-k}(y, x)$. Let $i = k + 1$. Then

$$\begin{aligned} W_i(x, y) &= W_{k+1}(x, y) \\ &= W_k(y, xy) \quad \text{by Property (i)} \\ &= W_{1-k}(xy, y) \quad \text{by inductive hypothesis} \\ &= W_{1-k}(W_{-1}(y, x), W_0(y, x)) \\ &= W_{-k}(y, x) \quad \text{by Property (i)} \\ &= W_{1-i}(y, x). \end{aligned}$$

Hence by induction $W_i(x, y) = W_{1-i}(y, x)$ holds for all $i \geqslant 0$.

If $i < 0$ let $i = 1 - j$ where $j > 1$. Then

$$W_i(x, y) = W_{1-j}(x, y) = W_j(y, x) = W_{1-i}(y, x).$$

So $W_i(x, y) = W_{1-i}(y, x)$ for all $i \in \mathbb{Z}$.

$$\begin{aligned}\text{(iv)}\ W_i(W_j(x, y), W_{j-1}(x, y)) &= W_{1-i}(W_{j-1}(x, y), W_j(x, y)) \quad \text{by Property (iii)}\\ &= W_{j-i}(x, y) \quad \text{by Property (i).}\end{aligned}$$

(v) We use induction to show that this is true for $i \geqslant 0$. The property holds for $i = 0$, 1 and 2. Assume it holds for $0 \leqslant i \leqslant k$. Then $W_{k+1}(x, x) = W_{k-1}(x, x) * W_k(x, x) = x * x = x$. Thus $W_i(x, x) = x$ for $i \geqslant 0$. Now if $i < 0$ then $1 - i > 0$ so $W_i(x, x) = W_{1-i}(x, x) = x$. □

Now for the first major theorem of this section.

Theorem 4.1. *Let m be a positive integer with $m \geqslant 6$ and let K be any subset of $\{1, 2, \ldots \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$. If*

- *$m \not\equiv 2 \pmod 4$ and*
- *for all integers t, $1 \leqslant t \leqslant m/2$ at least one of t, $t/2$ or $(m-t)/2 \in K$*

then $\mathbf{C}_m^K$ is a variety and a defining set of identities is

$$\begin{aligned} x^2 &= x,\\ (xy)y &= x,\\ W_m(x, y) &= x,\\ x\backslash_k W_k(x, y) &= y \quad \textit{for all } k \in K,\\ W_k(x, x\backslash_k y) &= y \quad \textit{for all } k \in K.\end{aligned}$$

Proof. Firstly we need to show that $\mathbf{C}_m^K$ satisfies these equations, but this just follows from the discussion in Section 1 because the algebras in $\mathbf{C}_m^K$ arise from K-perfect m-circuit systems. Conversely, we need to show that any algebra $(S, *, \backslash_K)$ which satisfies these identities arises from a K-perfect m-cycle system on S. Define a collection $\mathscr{C}$ of circuits by

$$\mathscr{C} = \{(W_0(a, b), W_1(a, b), W_2(a, b), W_3(a, b), \ldots, W_{m-1}(a, b)) \mid a \neq b \in S\}.$$

For brevity we write $W_i(a, b)$ as W_i from now on. We want to show that $(S, \mathscr{C})$ is a K-perfect m-cycle system.

Firstly we show that $\mathscr{C}$ is a set of m-cycles. Let $(W_0, W_1, \ldots, W_{m-1}) \in \mathscr{C}$ and suppose $W_0, W_1, \ldots, W_{m-1}$ are not all distinct. Then there exist $i \in \{0, 1, \ldots, m-1\}$ and $j \in \{1, \ldots, \lfloor m/2 \rfloor\}$ such that $W_i = W_{i+j}$. If $j = 1$ then $W_i * W_{i+1} = W_{i+2}$, so then $W_{i+1} * W_{i+2} = W_{i+3}$ and so it follows that

$$W_i = W_{i+1} = W_{i+2} = \cdots = W_m = a = W_{m+1} = b$$

which is a contradiction as $a \neq b$. If $j = 2$ then

$$\begin{aligned} W_{i+1-\lfloor m/2 \rfloor} &= W_{\lfloor m/2 \rfloor}(W_{i+1}, W_i) \quad \text{(by Lemma 4.1 (iv))}\\ &= W_{\lfloor m/2 \rfloor}(W_{i+1}, W_{i+2})\\ &= W_{i+1+\lfloor m/2 \rfloor} \quad \text{(by Lemma 4.1(i)).}\end{aligned}$$

Now if m is odd then

$$\begin{aligned} W_{i+1+\lfloor m/2 \rfloor} &= W_{i+1-\lfloor m/2 \rfloor} \quad \text{(from above)}\\ &= W_{i+1-(m-1)/2}\\ &= W_{i+1+(m+1)/2} \quad \text{(by Lemma 4.1(ii))}\\ &= W_{i+2+(m-1)/2}\\ &= W_{i+2+\lfloor m/2 \rfloor}.\end{aligned}$$

But from this we can conclude that $a = b$ (similarly to the case $j = 1$), thus m is even. Now at least one of 4, 2 or $(m-4)/2 \in K$ so K contains an even element say $2l$. Then

$$\begin{aligned} W_{2l}(W_{i+1-l}, W_{i+2-l}) &= W_{i+1+l} \quad \text{(by Lemma 4.1(i))} \\ &= W_l(W_{i+1}, W_{i+2}) \quad \text{(by Lemma 4.1(i))} \\ &= W_l(W_{i+1}, W_i) \\ &= W_{i+1-l} \quad \text{(by Lemma 4.1(iv))} \\ &= W_{2l}(W_{i+1-l}, W_{i+1-l}) \quad \text{(by Lemma 4.1(v)).} \end{aligned}$$

Thus either $W_{i+1-l} = W_{i+2-l}$ from which we can conclude that $a = b$ which is a contradiction, or that $2l \notin K$ which is a contradiction, so $j \neq 2$.

Thus $j \in \{3, \ldots, \lfloor m/2 \rfloor\}$. Now

$$\begin{aligned} W_j(W_i, W_{i+1}) &= W_{i+j} \quad \text{(by Lemma 4.1(i))} \\ &= W_i \\ &= W_j(W_i, W_i) \quad \text{(by Lemma 4.1(v))} \end{aligned}$$

implies that $j \notin K$. If j is odd then clearly $j/2 \notin K$. If j is even then

$$\begin{aligned} W_{j/2}(W_{i+j/2}, W_{i+(j/2)-1}) &= W_i \quad \text{(by Lemma 4.1(iv))} \\ &= W_{i+j} \\ &= W_{j/2}(W_{i+j/2}, W_{i+(j/2)+1}) \quad \text{(by Lemma 4.1(v)).} \end{aligned}$$

Thus either $W_{i+(j/2)-1} = W_{i+(j/2)+1}$ or $j/2 \notin K$. But the former leads to a contradiction similarly to the $j = 2$ case. So $j/2 \notin K$.

If $m - j$ is odd then clearly $(m-j)/2 \notin K$. If $m - j$ is even then

$$\begin{aligned} W_{(m-j)/2}(W_{i-(m-j)/2}, W_{i-(m-j)/2+1}) &= W_i \quad \text{(by Lemma 4.1(i))} \\ &= W_{i+j} \\ &= W_{(m-j)/2}(W_{i+(m+j)/2}, W_{i+(m+j)/2-1}) \quad \text{(by Lemma 4.1(iv))} \\ &= W_{(m-j)/2}(W_{i-(m-j)/2}, W_{i-(m+j)/2-1}) \quad \text{(by Lemma 4.1(iii)).} \end{aligned}$$

Then either $W_{i-(m-j)/2+1} = W_{i-(m-j)/2-1}$ or $(m-j)/2 \notin K$. But the former leads to a contradiction similarly to the $j = 2$ case. So $(m-j)/2 \notin K$.

But then j, $j/2$ and $(m-j)/2 \notin K$ which is a contradiction. So $(W_0, W_1, \ldots, W_{m-1})$ contains no repeats, hence $(W_0, W_1, \ldots, W_{m-1})$ is an m-cycle.

Now we show that $(S, \mathscr{C})$ is an m-cycle system. Clearly every edge in the cycle $(W_0(a,b), W_1(a,b), W_2(a,b), \ldots, W_{m-1}(a,b))$ generates the same cycle by the definition of W_i and the fact that $W_m(a,b) = a$. So an edge ab cannot be in two different cycles. Furthermore, every edge ab will be in some cycle in $\mathscr{C}$. So $(S, \mathscr{C})$ is an m-cycle system.

Finally we show that $(S, \mathscr{C})$ is K-perfect. Given distinct a and b in S and $k \in K$ let $c = a \backslash_k b$ and $C = (W_0(a,c), W_1(a,c), W_2(a,c), \ldots, W_{m-1}(a,c))$. Then $C(k)$ contains the edge ab. Furthermore, no other graph in $\mathscr{C}(k)$ can contain the edge ab as $\backslash_k$ is well defined. So $\mathscr{C}(k)$ partitions the edge set of the complete graph on S and $(S, \mathscr{C})$ is k-perfect. Since k is an arbitrary element of K, $(S, \mathscr{C})$ is K-perfect. Clearly $(S, \mathscr{C})$ gives rise to the algebra $(S, *, \backslash_K)$. □

We now prove the converse of the above theorem:

Theorem 4.2. *Let m be a positive integer with $m \geqslant 6$ and let K be any subset of $\{1, 2, \ldots, \lfloor (m-1)/2 \rfloor\}$ with $1 \in K$. If either*:

(i) $m \equiv 2 \pmod 4$ *or*
(ii) *there is an integer t, $1 \leqslant t \leqslant m/2$, such that t, $t/2$ and $(m-t)/2 \notin K$*

then $\mathbf{C}_m^K$ is not a variety.

Proof. First suppose $m \equiv 2 \pmod 4$. Then by Corollary 2.3 there is a finite K-perfect $(m/2, m/2)$-hourglass system. By Theorem 3.1 there is a K-perfect m-cycle system which gives rise to an algebra with a homomorphism onto the algebra arising from this K-perfect $(m/2, m/2)$-hourglass system. Now suppose there is an integer t, $1 \leqslant t \leqslant m/2$, such that t, $t/2$ and $(m-t)/2 \notin K$. Since $1 \in K$, $3 \leqslant t \leqslant m/2$. Thus by Corollary 2.3 there is a finite K-perfect $(t, m-t)$-hourglass system. By Theorem 3.1 there is a K-perfect m-cycle system which gives rise to an algebra with a homomorphism onto the algebra arising from this K-perfect $(t, m-t)$-hourglass system.

Finally we show that algebras arising from $(t, m-t)$-hourglass systems cannot arise from m-cycle systems. Because of the results proven in the previous paragraph, this implies that $\mathbf{C}_m^K$ is not closed under the taking of homomorphic images and hence is not a variety. Given a specific integer t, with $3 \leqslant t \leqslant m/2$, algebras arising from m-cycle systems have the property that $W_t(x, y) = x$ implies $x = y$. Algebras arising from $(t, m-t)$-hourlgass systems, however, do not have this property for if $(v_1, \ldots, v_t, v_1, v_{t+1}, \ldots, v_{m-1})$ is a $(t, m-t)$-hourglass in a $(t, m-t)$-hourglass system then $W_t(v_1, v_2) = v_1$. Thus, in no case does an algebra arising from a $(t, m-t)$-hourglass system also arise from an m-cycle system. We conclude that $\mathbf{C}_m^K$ is not closed under homomorphic images and hence is not a variety. □

Theorems 4.1 and 4.2 prove Theorem 1.1 for $m \geqslant 6$. For $m \in \{3, 4, 5\}$ the result for $K = \{1\}$ follows from [5] and for $K = \{1, 2\}$ from [6].

Acknowledgement

This research was supported by the Australian Research Council.

References

[1] G. Birkhoff, On the structure of abstract algebras, Proc. Cambridge Philos. Soc. 31 (1935) 433–454.
[2] D.E. Bryant, Varieties of P-quasigroups, Australas. J. Combin. 6 (1992) 229–243.
[3] D.E. Bryant, Varieties of quasigroups arising from 2-perfect m-cycle systems, Des. Codes Cryptogr. 2 (1992) 159–168.
[4] D.E. Bryant, Decompositions of directed graphs with loops and related algebras, Ars Combin. 38 (1994) 129–136.
[5] D.E. Bryant, A note on varieties of groupoids arising from m-cycle systems, J. Algebraic Combin. 4 (1995) 197–200.
[6] D.E. Bryant, C.C. Lindner, 2-perfect m-cycle systems can be equationally defined for $m = 3, 5$ and 7 only, Algebra Universalis 35 (1) (1996) 1–7.
[7] D.E. Bryant, C.C. Lindner, 2-perfect directed m-cycle systems can be equationally defined for $m = 3, 4$ and 5 only, J. Statist. Plann. Inference 56 (1996) 57–63.
[8] A. Kotzig, Groupoids and partitions of complete graphs, in: Combinatorial Structures and their Applications, Proceedings of Calgary International Conference Calgary Alta., Gordon and Breach, New York, 1970, pp. 215–221.
[9] C.C. Lindner, Graph theory and universal algebra go hand in hand, Austral. Math. Soc. Gaz. 24 (5) (1997) 191–215.
[10] C.C. Lindner, C.A. Rodger, On equationally defining m-perfect $2m + 1$ cycle systems, J. Combin. Des. 2 (5) (1994) 301–309.
[11] C.C. Lindner, C.A. Rodger, 2-perfect m-cycle systems, Discrete Math. 104 (1) (1994) 83–90.
[12] E.M. Li Marzi, C.C. Lindner, F. Rania, R.M. Wilson, {2, 3}-perfect m-cycle systems are equationally defined for $m = 5, 7, 8, 9$ and 11 only, J. Combin. Des. 12 (2004) 449–458.
[13] R.M. Wilson, Concerning the number of mutually orthogonal latin squares, Discrete Math. 9 (1974) 181–198.